UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/789,809	02/27/2004	Trevor W. Freeman	MS1-1747US	5655

22801 7590 06/26/2007

LEE & HAYES PLLC
421 W RIVERSIDE AVENUE SUITE 500
SPOKANE, WA 99201

EXAMINER	
KAPLAN, BENJAMIN A	

ART UNIT	PAPER NUMBER
2109	

NOTIFICATION DATE	DELIVERY MODE
06/26/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

lhptoms@leehayes.com

Office Action Summary	Application No.	Applicant(s)	
	10/789,809	FREEMAN ET AL.	
	Examiner	Art Unit	
	Benjamin A. Kaplan	2109	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 February 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-34* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-34* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *27 February 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *2/27/04 6/27/05 11/01/05*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-34 are pending.

Abstract

The abstract line 2 "generating public and private values one at least one appliance" is objected to, it is the examiners belief that the line was intended to be "generating public and private values one on at least one appliance". Please correct or clarify.

Claim Rejection/Objection - 35 USC § 112

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claim 29 is rejected/objected under 35 U.S.C. 112, second paragraph. Claim 29 lines 1-2 refers limitations regarding to "the out-of-band mechanism", however in Claim 29's parent claim, Claim 23 line 5 the mechanism was referred to as an "asynchronous mechanism". The mechanism should be referred to by the same name in both claims.

Claim Rejections - 35 USC § 101

4. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 9-34 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claims 9-15 are non-statutory because the computer readable medium can be any medium and in the specification paragraph [0055] specifically mentions signals, which are non-statutory.

Claims 16-34 are non-statutory because they recite a computer program per se representing functional descriptive material without a computer or computer readable medium.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1,2,3,6,7,8,9,10,11,14,15,16,17,18,19,22,30,31 and 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Enhanced IP Services for Cisco Networks (Cisco). In further view of C.O.B.A.S. Centralized Out-Of-Band Authentication System (C.O.B.A.S.).

As per Claim 1: Cisco teaches:

- A method for establishing a trust relationship with a remote node

(Cisco, Page 1, Paragraph 1, Lines 1-4 "IPsec is a fairly large collection of technologies that encompasses network and security protocols, cryptographic algorithms, and recommendations. IPsec is an architecture for building secure communications over untrusted networks and provides the security services listed in the following sections. These services are confidentiality, integrity, origin authentication, and anti-replay.").

- generating a local public value and a local private value on at least one node

(Cisco, Page 3, Line 31 "Alice and Bob are given numbers g and n. These are non-secret, publicly available numbers.").

(Cisco, Page 3, Lines 32-33 "Alice picks a large random number, x, calculates $A=g^x \bmod n$, and sends this value, A, to Bob over an untrusted network. The value x is known only to Alice and is called Alice's secret.").

At the Alice node, g is the public value and x is the private value.

- receiving a public value from another node

(Cisco, Page 3, Lines 34-35 "Bob picks a large random number, y, calculates $B=g^y \bmod n$, and sends this value, B, to Alice over the untrusted network. The value y is known only to Bob and is Bob's secret.").

At the Alice node, B is the public value received from the other node.

- and generating a secret value using the local private value in combination with the public value received from the other node.

(Cisco, Page 3, Line 36 "Alice computes $K_a = B^x \bmod n$.").

At the Alice node, the generated secret value is K_a.

Cisco does not explicitly teach:

- via an out-of-band mechanism

However C.O.B.A.S. in analogous art does teach the above limitation.

(C.O.B.A.S., Page 5, Paragraph 6 "The way to correct the fatal flaw is to separate the access and authentication paths. This can be done by having the authentication done via a separate network that the hacker does not have access to. This scheme is called Out-of-Band Authentication.").

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teachings of C.O.B.A.S in to the teachings of Cisco, because one of ordinary skill in the art would be motivated to protect or insulate authentication transactions such as key exchanges from interception, unauthorized monitoring and man in the middle attacks.

As per Claim 2: The rejection of claim 1 is incorporated and further Cisco teaches:

- method is performed on both of a pair of nodes

(Cisco, Page 3, Line 31 as seen in the rejection of claim 1).

(Cisco, Page 3, Lines 32-33 as seen in the rejection of claim 1).

(Cisco, Page 3, Lines 34-35 as seen in the rejection of claim 1).

(Cisco, Page 3, Line 37 "Bob computes $K_b = A^y \bmod n$.").

The corresponding values at the Bob node are: n is the public value, y is the private value, A is the public value received from the other node, K_b is the generated secret value.

- the secret values generated at both of the nodes are symmetric.

(Cisco, Page 3, Line 38 "By virtue of an algebraic property of exponents, K_a and K_b are equal").

As per Claim 3: The rejection of claim 2 is incorporated and further Cisco teaches:

- generating a secret value includes performing a Diffie-Hellman computation.

(Cisco, Page 3, Line 3 "Using Diffie-Hellman to Agree on a Shared Key").

The computations used in the rejections of claims 1 and 2 are Diffie-Hellman computations.

As per Claim 6: The rejection of claim 1 is incorporated and further Cisco does not explicitly teach:

- receiving of the public value from the other node via an out-of-band mechanism includes receiving the public value over an asynchronous connection.

However C.O.B.A.S. in analogous art does teach the above limitation.

Inherent as noted by applicant paragraph [0017] lines 3-4 "out-of-band, i.e., asynchronous".

As per Claim 7: The rejection of claim 1 is incorporated and further C.O.B.A.S. teaches:

- the receiving of the public value from the other node via an out-of-band mechanism includes downloading the public value from an external device

(C.O.B.A.S., Page 4, Lines 18-21 "The secret key can be stored on the user's computer or in a special hardware device called a "Token". A special case of a Token is a "Smart Card" which is a credit card sized plastic card with a microprocessor chip embedded in the card. Smart Cards require a reader on the computer where access is made.").

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teachings of C.O.B.A.S in to the teachings of Cisco, because one of ordinary skill in the art would be motivated to protect or insulate authentication transactions such as key exchanges from interception, unauthorized monitoring and man in the middle attacks.

As per Claim 8: The rejection of claim 7 is incorporated and further C.O.B.A.S. teaches:

- external device is any one of a personal digital assistant (PDA), flash memory, memory stick, barcode, smart card, USB-compatible device, Bluetooth-compatible device, and infrared-compatible device.

(C.O.B.A.S., Page 4, Lines 18-21 as seen in the rejection of claim 7).

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teachings of C.O.B.A.S in to the teachings of Cisco, because one of ordinary skill in the art would be motivated to protect or insulate authentication transactions such as key exchanges from interception, unauthorized monitoring and man in the middle attacks.

As per Claim 9: Claim 9 is the method claim of claim 1 as a computer readable medium and is rejected under the same reasons as set forth in the rejection of claim 1.

As per Claim 10: The rejection of claim 9 is incorporated and further:

Claim 10 is the method claim of claim 2 as a computer readable medium and is rejected under the same reasons as set forth in the rejection of claim 2.

As per Claim 11: The rejection of claim 9 is incorporated and further:

Claim 11 is the method claim of claim 3 as a computer readable medium and is rejected under the same reasons as set forth in the rejection of claim 3.

As per Claim 14: The rejection of claim 9 is incorporated and further:

Claim 14 is the method claim of claim 6 as a computer readable medium and is rejected under the same reasons as set forth in the rejection of claim 6.

As per Claim 15: The rejection of claim 9 is incorporated and further:

Claim 15 is the combination of the method claim of claim 7 and its dependent claim, claim 8 as a computer readable medium and is rejected under the same reasons as set forth in the rejection of claims 7 and 8.

As per Claim 16: Claim 16 is the method claim of claim 1 as an apparatus and is rejected under the same reasons as set forth in the rejection of claim 1.

As per Claim 17: The rejection of claim 16 is incorporated and further:

Claim 17 is the method claim of claim 16 as an apparatus and is rejected under the same reasons as set forth in the rejection of claim 16.

As per Claim 18: The rejection of claim 16 is incorporated and further Cisco teaches:

- the other node is a server

(Cisco, Page 2, Lines 25-28 "Alice and Bob represent any two parties that need to communicate securely over an untrusted infrastructure. Depending on the implementation, they can be people with PCs (or other client devices) or they can represent networking devices such as servers, routers, and firewalls (for instance, router Alice communicating with firewall Bob).").

As per Claim 19: The rejection of claim 16 is incorporated and further:

Claim 19 is the method claim of claim 3 as an apparatus and is rejected under the same reasons as set forth in the rejection of claim 3.

As per Claim 22: The rejection of claim 16 is incorporated and further:

Claim 22 is the method claim of claim 8 as an apparatus and is rejected under the same reasons as set forth in the rejection of claim 8.

As per Claim 30: Claim 30 is the method claim of claim 1 as an apparatus and is rejected under the same reasons as set forth in the rejection of claim 1.

As per Claim 31: The rejection of claim 30 is incorporated and further:

Claim 31 is the method claim of claim 3 as an apparatus and is rejected under the same reasons as set forth in the rejection of claim 3.

As per Claim 34: The rejection of claim 30 is incorporated and further:

Claim 34 is the method claim of claim 8 as an apparatus and is rejected under the same reasons as set forth in the rejection of claim 8.

7. Claims 1,4,5,6,7,8,9,12,13,14,15,16,18,20,21,22,30,32,33 and 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pretty Good Privacy™ PGP for Personal Privacy, Version 5.0 (PGP). In further view of Cisco and C.O.B.A.S..

As per Claim 1: PGP teaches:

- A method for establishing a trust relationship with a remote node

(PGP, Page 1, Lines 1-3 "With PGP™ for Personal Privacy, you can easily protect the privacy of your email messages and file attachments by encrypting them so that only those with the proper authority can decipher the information.").

- generating a local public value and a local private value on at least one node

(PGP, Page 3, Lines 9-10 "you need to generate a key pair consisting of a private key to which only you have access and a public key").

The public key is the public value; the private key is the private value.

- receiving a public value from another node

(PGP, Page 3, Lines 16-21 "After you have created a key pair, you can begin corresponding with other PGP users. To do so, you will need a copy of their public key

and they will need a copy of your public key. Since your public key is just a block of text, it is really quite easy to trade keys with someone. You can either include your public key in an email message, copy it to a file or you can post it on a public key server where anyone can get a copy when they need it.").

The public key that is sent from an "other PGP user" is the received public value.

PGP does not explicitly teach:

- and generating a secret value using the local private value in combination with the public value received from the other node.

However Cisco in analogous art teaches the above limitation.

(Cisco, Page 3, Line 36 "Alice computes $K_a = B^X \bmod n$.").

The generated secret value is K_a, X is the local private value, B is the public value from other node.

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teachings of PGP in to the teachings of Cisco, because one of ordinary skill in the art would be motivated to include a cryptographically strong equation in the generation of a pseudo-random single-key/session key.

PGP and Cisco do not explicitly teach:

- via an out-of-band mechanism

However C.O.B.A.S. in analogous art does teach the above limitation.

(C.O.B.A.S., Page 5, Paragraph 6 "The way to correct the fatal flaw is to separate the access and authentication paths. This can be done by having the authentication done via a separate network that the hacker does not have access to. This scheme is called Out-of-Band Authentication.").

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teachings of C.O.B.A.S in to the teachings of Cisco, because one of ordinary skill in the art would be motivated to protect or insulate authentication transactions such as key exchanges from interception, unauthorized monitoring and man in the middle attacks.

As per Claim 4: The rejection of claim 1 is incorporated and further PGP teaches:

- retaining the secret value locally

It is inherently necessary to retain the secret value (single-key/session key) in order to take any further action using it or based on it.

- protecting the secret value using the public value received from the other node

(PGP, Page 21, Lines 17-19 "the data is encrypted using a much faster single-key algorithm, and it is this single key that is actually encrypted using the recipients public key.").

- transmitting the protected secret value to the other node

(PGP, Page 22, Lines 26-58 "Unless you have already done so while using another version of PGP, the first thing you need to do before sending or receiving encrypted and certified e-mail is create a new key pair.").

(PGP, Page 22, Lines 2-5 "Anyone who has a copy of your public key can check your digital signature to confirm that you are the originator of the mail and that the contents have not been altered in any way during transit.").

PGP does not explicitly teach:

- via an out-of-band mechanism

However C.O.B.A.S. in analogous art does teach the above limitation.

(C.O.B.A.S., Page 5, Paragraph 6 as seen in the rejection of claim 1)

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teachings of C.O.B.A.S in to the teachings of Cisco, because one of ordinary skill in the art would be motivated to protect or insulate authentication transactions such as key exchanges from interception, unauthorized monitoring and man in the middle attacks.

As per Claim 5: The rejection of claim 4 is incorporated and further PGP teaches:

- the generating a secret value includes performing a Rivest-Shamir-Adleman (RSA) computation.

(PGP, Page 22, Lines 2-5 "This version of PGP supports two distinct types of keys—the traditional RSA key used in older versions of PGP").

As per Claim 6: The rejection of claim 1 is incorporated and further PGP does not explicitly teach:

- receiving of the public value from the other node via an out-of-band mechanism includes receiving the public value over an asynchronous connection.

However C.O.B.A.S. in analogous art does teach the above limitation.

Inherent as noted by applicant paragraph [0017] lines 3-4 "out-of-band, i.e., asynchronous".

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teachings of C.O.B.A.S in to the teachings of Cisco, because one of ordinary skill in the art would be motivated to protect or insulate authentication transactions such as key exchanges from interception, unauthorized monitoring and man in the middle attacks.

As per Claim 7: The rejection of claim 1 is incorporated and further PGP does not explicitly teach:

- the receiving of the public value from the other node via an out-of-band mechanism includes downloading the public value from an external device

However C.O.B.A.S. in analogous art does teach the above limitation.

(C.O.B.A.S., Page 4, Lines 18-21 "The secret key can be stored on the user's computer or in a special hardware device called a "Token". A special case of a Token is a "Smart Card" which is a credit card sized plastic card with a microprocessor chip embedded in the card. Smart Cards require a reader on the computer where access is made.").

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teachings of C.O.B.A.S in to the teachings of Cisco, because one of ordinary skill in the art would be motivated to protect or insulate authentication transactions such as key exchanges from interception, unauthorized monitoring and man in the middle attacks.

As per Claim 8: The rejection of claim 7 is incorporated and further PGP does not explicitly teach:

- external device is any one of a personal digital assistant (PDA), flash memory, memory stick, barcode, smart card, USB-compatible device, Bluetooth-compatible device, and infrared-compatible device.

However C.O.B.A.S. in analogous art does teach the above limitation.

(C.O.B.A.S., Page 4, Lines 18-21 as seen in the rejection of claim 7).

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teachings of C.O.B.A.S in to the teachings of Cisco, because one of ordinary skill in the art would be motivated to protect or insulate

authentication transactions such as key exchanges from interception, unauthorized monitoring and man in the middle attacks.

As per Claim 9: Claim 9 is the method claim of claim 1 as a computer readable medium and is rejected under the same reasons as set forth in the rejection of claim 1.

As per Claim 12: The rejection of claim 9 is incorporated and further:

Claim 12 is the method claim of claim 4 as a computer readable medium and is rejected under the same reasons as set forth in the rejection of claim 4.

As per Claim 13: The rejection of claim 12 is incorporated and further:

Claim 13 is the method claim of claim 5 as a computer readable medium and is rejected under the same reasons as set forth in the rejection of claim 5.

As per Claim 14: The rejection of claim 9 is incorporated and further:

Claim 14 is the method claim of claim 6 as a computer readable medium and is rejected under the same reasons as set forth in the rejection of claim 6.

As per Claim 15: The rejection of claim 9 is incorporated and further:

Claim 15 is the combination of the method claim of claim 7 and its dependent claim, claim 8 as a computer readable medium and is rejected under the same reasons as set forth in the rejection of claims 7 and 8.

As per Claim 16: Claim 16 is the method claim of claim 1 as an apparatus and is rejected under the same reasons as set forth in the rejection of claim 1.

As per Claim 18: The rejection of claim 16 is incorporated and further:

- the other node is a server

(Cisco, Page 2, Lines 25-28 "Alice and Bob represent any two parties that need to communicate securely over an untrusted infrastructure. Depending on the implementation, they can be people with PCs (or other client devices) or they can represent networking devices such as servers, routers, and firewalls (for instance, router Alice communicating with firewall Bob).").

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teachings of Cisco in to the teachings of PGP, because one of ordinary skill in the art would be motivated to have secure communications between different networked devices, including servers.

As per Claim 20: The rejection of claim 16 is incorporated and further:

Claim 20 is the method claim of claim 4 as an apparatus and is rejected under the same reasons as set forth in the rejection of claim 4.

As per Claim 21: The rejection of claim 20 is incorporated and further:

Claim 21 is the method claim of claim 5 as an apparatus and is rejected under the same reasons as set forth in the rejection of claim 5.

As per Claim 22: The rejection of claim 16 is incorporated and further:

Claim 22 is the method claim of claim 8 as an apparatus and is rejected under the same reasons as set forth in the rejection of claim 8.

As per Claim 30: Claim 30 is the method claim of claim 1 as an apparatus and is rejected under the same reasons as set forth in the rejection of claim 1.

As per Claim 32: The rejection of claim 30 is incorporated and further PGP teaches:

- means for encoding the shared secret using the public key received from the other node.

(PGP, Page 21, Lines 17-19 "the data is encrypted using a much faster single-key algorithm, and it is this single key that is actually encrypted using the recipients public key.").

Encrypting the single key inherently includes a means for encoding the shared secret (single key).

As per Claim 33: The rejection of claim 31 is incorporated and further:

Claim 33 is the method claim of claim 5 as an apparatus and is rejected under the same reasons as set forth in the rejection of claim 5.

As per Claim 34: The rejection of claim 30 is incorporated and further:

Claim 34 is the method claim of claim 8 as an apparatus and is rejected under the same reasons as set forth in the rejection of claim 8.

8. Claims 23,27,28 and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over PGP in further view of C.O.B.A.S..

As per Claim 23: PGP teaches:

- A protocol for establishing trust between two or more processing nodes

(PGP, Page 1, Lines 1-3 "With PGP™ for Personal Privacy, you can easily protect the privacy of your email messages and file attachments by encrypting them so that only those with the proper authority can decipher the information.").

- generating a public key and a private key on each of at least two nodes

(PGP, Page 21, Lines 6-8 "PGP is based on a widely accepted and highly trusted "public key encryption" system by which you and other PGP users generate a key pair consisting of a private key and a public key.").

- exchanging the public keys between the at least two nodes

(PGP, Page 21, Lines 9-11 "in order to correspond with other PGP users you need a copy of their public key and they need a copy of your public key.").

This inherently involves exchanging public keys.

- calculating a secret to be shared on at least one of the two nodes

(PGP, Page 91, Lines 12-13 "PGP uses a cryptographically strong pseudo-random number generator for creating temporary session keys.").

PGP does not explicitly teach:

- using an asynchronous mechanism

However C.O.B.A.S. in analogous art does teach the above limitation.

(C.O.B.A.S., Page 5, Paragraph 6 as seen in the rejection of claim 1)

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teachings of C.O.B.A.S in to the teachings of Cisco, because one of ordinary skill in the art would be motivated to protect or insulate authentication transactions such as key exchanges from interception, unauthorized monitoring and man in the middle attacks.

As per Claim 27: The rejection of claim 23 is incorporated and further PGP teaches:

- encoding the secret to be shared using the public key from the other of the two nodes

(PGP, Page 21, Lines 17-19 "the data is encrypted using a much faster single-key algorithm, and it is this single key that is actually encrypted using the recipients public key.").

- transmitting the encoded secret to be shared to the other of the two nodes

(PGP, Page 22, Lines 26-58 "Unless you have already done so while using another version of PGP, the first thing you need to do before sending or receiving encrypted and certified e-mail is create a new key pair.").

(PGP, Page 22, Lines 2-5 "Anyone who has a copy of your public key can check your digital signature to confirm that you are the originator of the mail and that the contents have not been altered in any way during transit.").

PGP does not explicitly teach:

- via the asynchronous mechanism

However C.O.B.A.S. in analogous art does teach the above limitation.

(C.O.B.A.S., Page 5, Paragraph 6 as seen in the rejection of claim 1)

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teachings of C.O.B.A.S in to the teachings of Cisco, because one of ordinary skill in the art would be motivated to protect or insulate

authentication transactions such as key exchanges from interception, unauthorized monitoring and man in the middle attacks.

As per Claim 28: The rejection of claim 27 is incorporated and further PGP teaches:

- the calculating the secret to be shared includes performing an RSA calculation.

(PGP, Page 22, Lines 2-5 "This version of PGP supports two distinct types of keys—the traditional RSA key used in older versions of PGP").

As per Claim 29: The rejection of claim 23 is incorporated and further:

Claim 29 is the method claim of claim 8 as a protocol and is rejected under the same reasons as set forth in the rejection of claim 8.

9. Claims 24,25 and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over (PGP). In further view of Cisco and C.O.B.A.S..

As per claim 24: The rejection of claim 23 is incorporated and further:

PGP does not explicitly teach:

- the calculating of the secret to be shared includes performing a function using the public key from the other of the two nodes and the private key.

However Cisco in analogous art teaches the above limitation.

(Cisco, Page 3, Line 36 "Alice computes $K_a = B^x \bmod n$.").

The generated secret value is K_a, X is the local private Key, B is the public key from other node.

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teachings of Cisco in to the teachings of PGP and C.O.B.A.S., because one of ordinary skill in the art would be motivated to include a cryptographically strong equation in the generation of a pseudo-random single-key/session key.

As per claim 25: The rejection of claim 24 is incorporated and further PGP teaches:

- the calculating the secret to be shared includes performing a Diffie-Hellman calculation.

(PGP, Page 88, Lines 4-5 "PGP gives you the option of using keys based on the DSS/Diffie-Hellman encryption").

As per claim 26: The rejection of claim 24 is incorporated and further PGP teaches:

- the secret to be shared is symmetrical on the at least two nodes

(PGP, Page 88, Lines 9-13 "The PGP Symmetric Algorithms PGP offers a selection of different secret-key algorithms to encrypt the actual message. By secret key

algorithm, we mean a conventional, or symmetric, block cipher that uses the same key to both encrypt and decrypt.").

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Benjamin A. Kaplan whose telephone number is 571-270-3170. The examiner can normally be reached on 7:30 a.m. - 5:00 p.m. E.S.T..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Chameli Das can be reached on 571-272-3696. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Benjamin Kaplan

Chameli Das
CHAMELI DAS
SUPERVISORY PATENT EXAMINER
6/19/07.